HAYNES AND BOONE, LLP
Kenneth G. Parker / Bar No. 182911
kenneth.parker@haynesboone.com
Thomas B. King / Bar No. 241661
thomas.king@haynesboone.com
600 Anton Boulevard, Suite 700
Costa Mesa, California 92626
Telephone: (949) 202-3000
Facsimile (949) 202-3001

Attorneys for Plaintiff
mSIGNIA, Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MSIGNIA, INC., a California corporation,

Plaintiff,

v.

INAUTH, INC., a Delaware corporation,

Defendant.

Case No. 8:17-cv-1289

COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

Plaintiff mSIGNIA, Inc. ("mSIGNIA", or "Plaintiff") hereby brings this action against Defendant InAuth, Inc. ("InAuth", or "Defendant") and alleges as follows upon actual knowledge with respect to itself and its own acts, and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is a civil action for patent infringement.

2. mSIGNIA is the legal owner by assignment of U.S. Patent No. 9,559,852 ("the '852 Patent"), which was duly and legally issued by the United States Patent and Trademark Office ("USPTO").

3. mSIGNIA provides computer security products to businesses who need to authenticate users and devices. mSIGNIA's products are based on technology that is described and claimed in the '852 patent. mSIGNIA's patented offerings include its iDNA and 3D Secure products.

4. Defendant InAuth also sells products for authenticating users and devices, including products based on the so-called "InAuth Security Platform." However, as set forth below, the InAuth Security Platform infringes one or more claims of the '852 patent, as do any products, systems, and services related to the InAuth Security Platform and other related InAuth products that use or relate to components of the InAuth Security Platform ("Infringing Products"). InAuth's Infringing Products include but are not limited to InMobile, InBrowser, InRisk, InAuthenticate, InExchange, InReach, InPermID, and other products that use the InAuth Security Platform.

5. mSIGNIA brings this action to remedy InAuth's infringement. mSIGNIA seeks injunctive relief and monetary damages as set forth below.

THE PARTIES

6. mSIGNIA is a corporation organized and existing under the laws of California, with its principal office located at 109 Holiday Court, Suite D7, Franklin, TN 37067. Paul Miller, mSIGNIA's co-founder, Chief Executive Officer

and Secretary, resides and works out of this District, at 10 Wandering Rill, Irvine, CA 92603.

7. Upon information and belief, InAuth is a corporation organized and existing under the laws of the State of Delaware. InAuth claims to have a West Coast Office located at 227 Broadway, Suite 200, Santa Monica, CA 90401. (*See e.g.*, https://www.inauth.com/contact/.) Upon information and belief, InAuth's West Coast Office is focused at least in part on engineering and product development.

JURISDICTION AND VENUE

8. This is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*.

9. This Court has subject matter jurisdiction over the matters asserted pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over InAuth. InAuth has infringed the '852 patent in the Central District of California by, among other things, engaging in infringing conduct within and directed at or from this District, including, based on information and belief, by developing its Infringing Products out of an office in this District and by the advertisement, solicitation of customers, marketing, and distribution of services that practice the claims of the '852 Patent. For example, InAuth has purposefully and voluntarily sold one or more of its infringing products or services, as described below, into the stream of commerce with the expectation that these infringing products or services will be used in this District. These infringing products or services have been and continue to be used in this District.

11. Venue is proper in this district and division under 28 U.S.C. § 1400(b) at least because InAuth has a regular and established place of business in the Central District of California. Specifically, InAuth's West Coast Office is located at 227 Broadway, Suite 200, Santa Monica, CA 90401. (*See e.g.*,

https://www.inauth.com/contact/.) Moreover, InAuth has committed acts of infringement in this judicial district because, based on information and belief, InAuth's West Coast Office focuses on engineering and technical development, including the development of the Infringing Products, and as such, upon information and belief, InAuth has used the Infringing Products in this district. In addition, InAuth has developed its websites and services from its offices in this judicial district, and additionally, it has purposefully and voluntarily engaged in the making, using, selling, offering for sale, or importing in to the United States without authority, products, methods, equipment, or services that practice one or more claims of the '852 patent.

MSIGNIA'S PATENTED TECHNOLOGY

12. mSIGNIA was founded by Paul Miller and George Tuvell in October 2010. Mr. Miller is the Chief Executive Officer of mSIGNIA, and Mr. Tuvell is the current Chief Product Officer and former Chief Technology Officer. Both Mr. Miller and Mr. Tuvell are longtime experts in the field of authentication and computer security.

13. Online identity fraud has been a major problem for many years. Such fraud costs online retailers and banks billions of dollars per year in the United States and abroad. In 2010, a variety of technologies existed for combatting such identity fraud. These technologies are called "authentication" mechanisms. The most basic type of authentication involves the use of a user name and password. Another type of authentication requires the possession of digital "certificates." Another type of authentication recognizes the device of a user. Yet another type of authentication involves the use of "biometrics" (e.g., a fingerprint scanner).

14. Each of these prior art technologies suffers from some well-known drawbacks. Simple passwords can be easily stolen or guessed by computer programs. Alternatively, passwords may become too complicated in which case they are easily forgotten. Other technologies, such as digital certificates and

device recognition, only confirm the identity of a device; they do not confirm the identity of the person using the device. And biometric authentication suffers from the problem that although a fingerprint may be unique, a digital representation of a fingerprint can be intercepted, copied or not available on a new device.

15. Because of these drawbacks, modern systems often use two or more forms of authentication. But many of these secondary authentication techniques are said to create customer "friction." In other words, they are hard for consumers to use. For example, many authentication technologies require the input of a randomly-generated code that is delivered by text message, by email address, or through a separate application. These authentication technologies create user frustration and, at least in the e-commerce setting, may actually prevent bona fide willing customers from completing a purchase.

16. By 2010, these problems were well-known and getting worse due to the rise of mobile handheld devices. Mobile devices generally do not have anti-virus technology installed, and their applications are designed for simplicity, not security. In fact, many mobile devices are not even protected by a password. At the same time, mobile device users expect their phones to "just work," and get frustrated by authentication technologies that unnecessarily block access to resources.

17. Thus, mobile devices presented a new challenge for combatting identity fraud, because they present an inherently unprotected environment in which users refused to accept the "friction" that was traditionally used to provide authentication.

18. The founders of mSIGNIA invented a new system that addressed these problems. Although mobile devices are insecure, they are also rich sources of information. In particular, mobile devices are highly customizable, such that shortly after purchase, each device is essentially unique to a user. Thus, a mobile device can be used to uniquely authenticate a user because the combination of data

values on the mobile device are unique to that user/device.

19. One major problem with this "device as fingerprint" idea is that device data values are subject to change. Unlike a person's fingerprint or DNA, data values on, e.g., a mobile device, change frequently, making it difficult to obtain a true "fingerprint" of the device. This dynamically changing data makes it especially difficult to apply prior art authentication techniques to mobile devices. However, mSIGNIA's founders realized that by applying complex algorithms and *anticipating* what the device data values *would be at a future time*, they could still use changing data from a device to perform authentication. This technique was also useful for encryption. Mr. Miller and Mr. Tuvell developed their technology ideas in 2010-2011, and filed a provisional patent application on February 3, 2011.

20. Around this time, Mr. Miller and Mr. Tuvell were looking for potential investors and others to help them commercialize their new technology. One of the individuals they contacted was Michael Patterson. Mr. Miller and Mr. Tuvell considered Mr. Patterson as a potential candidate to be mSIGNIA's first sales person, but they ultimately decided that he was unsuitable for the position. Shortly afterwards, Mr. Patterson contacted Mr. Miller and Mr. Tuvell asking them if *they* would be willing to invest in a new company named InAuth that *Mr. Patterson* was planning to form. Mr. Patterson provided them with an investment presentation. The presentation reflected many of the technical ideas and concepts that Mr. Miller and Mr. Tuvell had developed.

21. Recently, mSIGNIA learned that InAuth had not just adapted Mr. Miller and Mr. Tuvell's ideas for its 2011 investor proposals; InAuth had actually built its products around the ideas that mSIGNIA had developed. Further investigation revealed that InAuth was likely infringing a patent that mSIGNIA had recently obtained, U.S. Patent No. 9,559,852. mSIGNIA is bringing this patent lawsuit to vindicate those patent rights.

/ / /

COUNT 1: INFRINGEMENT OF THE '852 PATENT

22. The allegations of paragraphs 1-21 of this Complaint are incorporated by reference as though fully set forth herein.

23. One of mSIGNIA's patents, the '852 patent, was granted by the USPTO on January 31, 2017. The '852 patent is entitled "Cryptographic Security Functions Based on Anticipated Changes in Dynamic Minutiae." A true and correct copy of the '852 patent is attached hereto as Exhibit A.

24. Paul Timothy Miller and George Allen Tuvell are the named inventors of the '852 patent. mSIGNIA is the original and current owner of the '852 patent, and owns the entire right, title, and interest in the '852 patent.

25. The '852 patent is valid and enforceable.

26. The '852 patent generally relates to identifying and authenticating a user and their device by using dynamically changing data from a device, such as media, geolocation, call information, network information, etc.

27. As part of its sales literature, InAuth advertises that the Infringing Product gives its users the ability to "uniquely and consistently identify and authenticate mobile devices across time, users, and apps." The Infringing Product "leverages up to 2,000 device attributes" to allow a customer to "access [] a mobile app or website." According to InAuth, the goal of the Infringing Product is to "provide[] frictionless experiences for known good devices." (available at https://www.inauth.com/products/inauth-security-platform/).

28. InAuth has directly infringed and is currently directly infringing the '852 patent, literally or under the doctrine of equivalents, by making, using, selling, offering for sale, or importing in to the United States without authority, products, methods, equipment, or services that practice one or more claims of the '852 patent in connection with the Accused Product.

29. As a non-limiting example, set forth below (claim language in italics) is a description of infringement of exemplary claims 1 of the '852 patent in

connection with the Infringing Product. This description is based on publicly available information. mSIGNIA reserves the right to modify the description, including on the basis of information about the '852 patent that mSIGNIA obtains during discovery.

a. *[1.] An identity recognition system comprising:* The Infringing Products provide an identity recognition system. InAuth's website states that "[w]hen a customer accesses your mobile app or website, InAuth leverages up to 2,000 device attributes to consistently and uniquely identify it." *Source: https://www.inauth.com/products/inauth-security-platform/*

b. *[1.1.1] a non-transitory memory storing information associated with one or more identities:* On information and belief, the Infringing Products use a client-server system for identity authentication. The "memory storing information associated with one or more identities" is located on the server-side. InAuth collects device attributes and sends them to its servers. The device attributes that the Infringing Products collect include data from the device such as accelerometer, battery, contacts, data usage, GPS, hardware, media, process, phone, wifi, calendar, photos and twitter and device access data. Upon information and belief, collecting this information for large numbers of devices requires a non-transitory memory.

c. *[1.1.2] wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity:* The Infringing Products collects and stores dynamic data values associated with the identity of a mobile device. *See e.g.*, https://www.inauth.com/products/inauth-security-platform/ ("When a customer accesses your mobile app or

website, InAuth leverages up to 2,000 device attributes to consistently and uniquely identify it.") The Infringing Products collect device attributes such as accelerometer, battery, contacts, data usage, GPS, hardware, media, process, phone, wifi, calendar, photos and twitter and device access data. Most of these device attributes involve changing data. Upon information and belief, there is at least a reasonable likelihood that InAuth also stores data regarding anticipated changes to the device attributes that it has already collected. At one point in time, InAuth may have referred to such data about anticipated changes as being part of a "CR build." The ability to identify anticipated changes is also likely necessary to enable the Infringing Products to accomplish their stated purpose of using these changing data attributes to "consistently and uniquely" identify a device.

d. *[1.2] one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations comprising:* On information and belief, the Infringing Products use servers to authenticate with mobile devices, which necessarily include one or more hardware processors.

e. *[1.3] generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the stored data values associated with the identity:* As noted, the InAuth Security Platform collects device attributes from a device such as a mobile device. The Infringing Products prompt the device to provide a response to the server with updated versions of the collected device

attributes.

f. *[1.4] receiving, from the computer, the response to the challenge*: As noted, the Infringing Products collect device attributes from a device such as a mobile device. The Infringing Products prompt the device to provide those attributes as a response to a challenge.

g. *[1.5] determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value; and recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge*: Upon information and belief, InAuth's authentication process involves comparing data values that are received as part of the response to anticipated changes to corresponding stored data values. As noted, at one point in time, InAuth may have referred to such data about anticipated changes being part of a "CR build." InAuth or its privies then use this information to recognize whether the presentation of the identity is authentic.

PRAYER FOR RELIEF

WHEREFORE, mSIGNIA prays for the following relief:

1. A judgment:

a. that InAuth has infringed one or more claims of the '852 Patent, literally or under the doctrine of equivalents;

b. that, pursuant to 35 U.S.C. § 283, InAuth and its affiliates, employees, agents, officers, directors, attorneys, successors, assigns, and all those acting on or behalf of, or in active concert or participation with it, be

preliminary and permanently enjoined from (1) infringing the Asserted Patent, and (2) making, using, selling, and offering for sale the Accused Product;

c. Awarding damages sufficient to compensate mSIGNIA for Defendant's infringement under 35 U.S.C. § 284, and in any event no less than a reasonable royalty;

d. Finding this case and InAuth's infringement exceptional under 35 U.S.C. § 285 and awarding mSIGNIA treble damages as provided by 35 U.S.C. § 284;

e. That mSIGNIA be awarded its reasonable attorneys' fees in this action;

f. Awarding costs and expenses in this action;

g. Awarding prejudgment and post-judgment interest; and

2. Any and all such other relief that the Court may deem to be just and proper.

DATED: July 26, 2017

HAYNES AND BOONE, LLP

By: */s/ Kenneth G. Parker*
Kenneth G. Parker
Attorneys for Plaintiff,
mSIGNIA, Inc.

DEMAND FOR JURY TRIAL

mSIGNIA respectfully demands a trial by jury on all issues triable by jury.

DATED: July 26, 2017

HAYNES AND BOONE, LLP

By: */s/ Kenneth G. Parker*
Kenneth G. Parker
Attorneys for Plaintiff,
mSIGNIA, Inc.